electronics

MDPI

Article

Design of a Decentralized Identifier-Based Authentication and Access Control Model for Smart Homes

Xinyang Zhao *, Bocheng Zhong and Zicai Cui

School of Electronic of Electrical Engineering, Shanghai University of Engineering Science, Shanghai 201620, China; bczhong@sues.edu.cn (B.Z.); m020220344@sues.edu.cn (Z.C.)
* Correspondence: m025120514@sues.edu.cn

Abstract: In recent years, smart homes have garnered extensive attention as a prominent application scenario of IoT technology. However, the unique characteristics of smart homes have brought forth serious security threats, emphasizing the paramount importance of identity authentication and access control. The conventional centralized approach is plagued by the issue of having a "single point of failure," while existing distributed solutions are constrained by limited device resources and the complexities of identity authentication. To tackle these challenges, this paper proposes a smart home authentication and access control model based on decentralized identifiers (DIDs). By leveraging the inherent decentralization of DIDs, which rely on blockchain, a distributed environment is constructed, effectively mitigating the problem of the "single point of failure." In this model, every participant in the smart home system, including users and smart devices, is uniquely identified by DIDs and through the integration of an improved capability-based access control scheme, which streamlines the user identity authentication process, reduces authentication complexity, and enables convenient cross-household access with a single registration. Our experimental results demonstrate that the application of decentralized identifiers provides the model with various security attributes, including confidentiality, integrity, and traceability. Additionally, the model exhibits low time costs for each module, ensuring timely responses to access service requests and incurring lower gas consumption compared to other Ethereum-based methods. Thus, our research proposes a lightweight authentication and access control solution suitable for smart home environments.

Keywords: decentralized identifier; blockchain; access control; identity authentication

Citation: Zhao, X.; Zhong, B.; Cui, Z. Design of a Decentralized Identifier-Based Authentication and Access Control Model for Smart Homes. *Electronics* **2023**, *12*, 3334. https://doi.org/10.3390/electronics12153334

Academic Editor: Cheng-Chi Lee

Received: 5 July 2023
Revised: 28 July 2023
Accepted: 2 August 2023
Published: 4 August 2023

1. Introduction

Smart homes, domains of the Internet of Things (IoT) [1], involve the interconnection of various devices, appliances, and systems within households through intelligent devices and sensors [2]. This enables intelligent control and management. The average growth rate of smart homes and their equipment was more than 30%, from 500 million smart home applications to 700 million applications per year in the time interval of 2018–2022 [3]. However, with the increasing popularity and expanding scope of smart homes, the potential risks of malicious network attacks have been recognized to pose substantial threats to user security and privacy [4].

Firstly, devices in smart home systems are typically connected to the internet, making them susceptible to network attacks. Smart home systems can be remotely targeted by hackers through vulnerabilities or password cracking, allowing them to gain control or manipulate the functionalities of smart home devices. For example, attackers may exploit smart door locks or cameras to gain entry into homes or engage in intrusive surveillance of household members. Additionally, smart home devices often incorporate sensors and cameras that collect sensitive information about household members, which may be exposed to third-party applications and advertisers. For instance, smart home devices may store data on the schedules, preferences, and consumption habits of household members, which

could be utilized for advertising or targeted marketing, posing a threat to the personal privacy of household members.

In response to these security threats, identity authentication and access control have become critical security technologies in the field of smart homes. Identity authentication ensures that only authorized users can access smart home systems and devices, thus preventing unauthorized access and hacker attacks. Access control helps manage data and device usage permissions for household members, thereby limiting users' access to sensitive information. Among them, digital signatures play a crucial role and are an indispensable key component in modern computer systems and networks. In recent years, researchers have found that quantum technology holds the potential to provide stronger security measures, safeguarding information in smart homes, including digital payments, from computational attacks and data breaches. Schiansky et al. [5] introduced the use of quantum light to generate inherently unforgeable quantum cryptograms, ensuring the security of daily digital payments. Yin et al. [6] proposed an efficient quantum digital signature protocol with a higher signature efficiency and better security features. Pereira et al. [7] focused on addressing the security of the BB84 protocol in the presence of multiple source flaws by introducing a fourth state to improve system performance. Gu et al. [8] demonstrated the security of a laser-pulse-based four-phase measurement-device-independent quantum key distribution (QKD) protocol under potential source flaws using the reference technique and experimentally showed the feasibility of the protocol, along with its potential to enhance the secure key rate and transmission distance in the presence of device imperfections, showcasing its applicability in practical secure quantum key distribution.

In addition, various specific smart home authentication and access control schemes have been proposed by researchers; however, these schemes encounter certain challenges. For instance, password-based schemes are susceptible to threats such as password guessing and brute-force attacks, while biometric-based schemes pose risks of biometric data theft. Specifically, Kang et al. [9] proposed an enhanced security framework utilizing self-signature and access control techniques to mitigate security threats, including data tampering, leakage, and code forgery. However, the framework failed to consider the limited computational power and constrained resources of smart home devices, resulting in resource constraints and hindering their widespread adoption. Wu et al. [10] designed a provably secure authentication scheme that combines SGX and gateways to prevent internal attacks. However, in this scheme, users are required to set strong passwords and restrict access to smart devices, which may need further improvements to meet the growing security demands. Haseeb-ur-Rehman et al. [11] designed an authentication protocol for smart home environments, which outperforms previous state-of-the-art protocols in terms of security features, computation, and communication complexity. Nevertheless, the authors acknowledge that striking a balance between lightweightness and security in smart home authentication schemes remains a challenge.

The traditional centralized architecture [12] of access control schemes has facilitated the development of the security field in the domain of smart homes to a certain extent. However, these schemes commonly suffer from a shared vulnerability, namely, the lack of resistance against a "single point of failure." In a centralized system, if the central node fails, the entire system is affected, potentially leading to system breakdown and data loss. To address such issues, blockchain technology has gradually been employed in the field of Internet of Things (IoT) security. Blockchain is a distributed ledger technology that enables decentralized data storage and interaction. In a blockchain, each node possesses a complete copy of the ledger, and consensus algorithms are employed among the nodes to ensure data consistency and reliability. Due to the decentralized nature of blockchain, the system can continue to operate even if some nodes experience failures. For instance, Dorri et al. [13] proposed a blockchain-based secure lightweight smart home architecture, in which miners distribute shared keys to protect local devices and facilitate communication among coverage nodes, ensuring data confidentiality, integrity, and availability. Yakubu et al. [14] introduced a novel approach utilizing Diffie–Hellman key exchange, ECDLP, one-way hash functions,

blockchain, and smart contracts to protect the DHCP server in smart homes, thereby enhancing resilience against internal and external threats. Singh et al. [15] combined consortium blockchains with cloud computing, presenting a secure and efficient smart home architecture to achieve confidentiality, integrity, scalability, and availability, ensuring the security of smart homes. Menon et al. [16] proposed a learning engine for secure smart home communication networks, employing blockchain-based secure communication and cloud-based data evaluation layers to isolate and rank data, demonstrating superiority in terms of the computational complexity and error authentication rate compared to that of existing techniques. She et al. [17] designed a consortium blockchain-based smart home system, specifically optimized for data privacy. While the model was evaluated through performance simulations, further testing is required to assess metrics such as energy consumption and response time.

Although the introduction of blockchain technology has played a role in addressing security and privacy issues in smart homes, existing research still exhibits certain limitations. For instance, due to the limited resources of smart devices, many seemingly secure solutions are impractical to implement in real smart home environments. Alternatively, while some solutions take into account the resource constraints of smart devices, the design trade-off for enhanced security often results in repetitive and cumbersome identity authentication processes, leading to high time delays and inconveniences for users.

To enhance user experience, this paper introduces decentralized identifiers (DIDs) to address the balance between security and convenience in smart home systems. Firstly, DID technology can improve the speed and efficiency of identity verification, reducing the redundancy and time delays associated with authentication. Secondly, DID technology can effectively protect user privacy, preventing the disclosure and misuse of identity information. Most importantly, DID technology can mitigate the risk of single points of failure, making smart home systems more secure and reliable.

Therefore, in this paper, we propose a decentralized identifier-based authentication and access control model for smart homes. In our design, each participant in the smart home system, including users and smart devices, is identified by a unique DID. The access control for specific smart device services is determined by capability tokens. The main contributions of this paper are as follows:

- An innovative authentication and access control model for smart homes is proposed in this paper, leveraging the decentralized nature of decentralized identifiers (DIDs) to effectively address the issue of single points of failure in traditional solutions. This model enables multiple smart homes to connect to the same blockchain network, allowing users to register once and access across households, thereby overcoming the complexity of authentication processes in traditional solutions and enhancing user experience.
- To accommodate the proposed system model, we have improved the capability-based access control scheme and introduced two types of tokens for authorization. This approach leverages the advantages of decentralized identifiers while ensuring high security and responsiveness.
- A thorough analysis of the proposed model is conducted through experiments, comparing it with other approaches. The results demonstrate the lightweight, secure, and reliable nature of the proposed solution, making it highly suitable for addressing security requirements in smart home environments.

The remaining sections of this paper are organized as follows. In Section 2, we introduce the relevant background knowledge of this study. In Section 3, we present a blockchain-based security system model for smart homes. In Section 4, we propose a decentralized identifier-based authentication and access control scheme for smart home scenarios. In Section 5, we conduct a security and performance analysis of the proposed scheme. Finally, we summarize the paper in Section 6.

2. Relevant Information

2.1. Blockchain

Blockchain [18] technology is an emerging application paradigm based on distributed computing, peer-to-peer communication, consensus mechanisms, and encryption techniques. It fundamentally serves as a decentralized database that stores data in a chain-like structure, enabling data sharing and verification across multiple nodes, thus achieving decentralization, sharing, and trust. The core features of blockchain technology include immutability, security, transparency, decentralization, and autonomy.

As illustrated in Figure 1, the basic structure of a blockchain consists of a series of data blocks linked together. Each block comprises a block header and a block body. The block header typically includes metadata information such as the block's hash value, a timestamp, a random number, and the hash value of the previous block. The block body stores transaction data or other types of information, with each transaction encoded into a hash value and referenced by a Merkle tree root node in the block header. Consequently, the hash value of each block depends on its transaction data and the hash value of the previous block, thus forming an immutable chain-like structure.

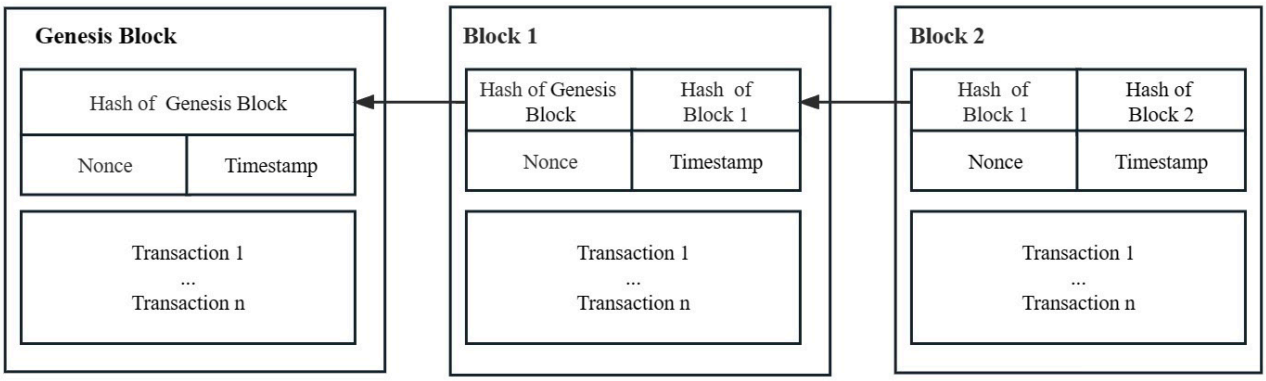

Figure 1. Blockchain structure.

2.2. Decentralized Identifiers

Decentralized identifiers [19] (DIDs) are digital identifiers used to identify individuals, organizations, or objects. They enable identity authentication and recognition without relying on any central authority. Unlike traditional authentication methods, DIDs are decentralized identity identifiers that do not require verification through centralized institutions or the provision of personal information by users, thereby safeguarding privacy and security.

A DID consists of a unique identifier and a set of metadata. The unique identifier is composed of a DID method and a specific string, representing the ownership and control of the DID. Users can generate different DIDs in various networks and use them for identity authentication and recognition. The implementation of DIDs relies on distributed ledger technologies, such as blockchain. DIDs can be combined with technologies such as smart contracts to achieve advanced levels of identity authentication and recognition [20].

In addition to the basic unique identifier and metadata information, a decentralized identifier (DID) also consists of a crucial component called the DID data object (DDO). The DDO serves as an extension to the DID and includes essential information such as public keys and service endpoints related to the DID. It is used to verify the ownership and control of the DID. The combination of DIDs and DDOs provides a secure, efficient, highly trustworthy, and privacy-preserving method for identity authentication and recognition. The DDO not only helps verify the ownership and control of the DID but also provides additional information to assist users in establishing trust relationships. Typically, the DDO is a JSON-formatted data object stored in a distributed ledger network.

2.3. Capability-Based Access Control

Capability-based access control (CBAC) is a secure access control mechanism that utilizes access tokens, also known as capabilities, to control a subject's access to resources [21]. Each token represents a specific access permission, and subjects can grant these tokens to other subjects as needed, thereby granting them corresponding access privileges.

The core idea of CBAC is to control access based on permissions or capabilities rather than identity or roles. It ensures that only subjects with the appropriate capabilities can access the corresponding resources. Each subject is granted a set of capabilities that authorize them to perform specific operations. When a subject wants to access a resource, it needs to provide the corresponding capability, instead of relying on traditional mechanisms of authentication and authorization [22]. The characteristics of CBAC allow for a high degree of flexibility and granular access control, as capabilities can be granted to any entity and provide precise control over resource access. Furthermore, CBAC can offer improved isolation and security by ensuring that each subject can only access the resources it is authorized for and restricting interactions between subjects.

2.4. Elliptic Curve Cryptography

The Elliptic Curve Integrated Encryption Scheme (ECIES) is a widely used public-key encryption algorithm for ensuring data privacy and security [23,24]. Its fundamental idea is to combine symmetric encryption and public-key encryption, providing enhanced security through elliptic curve cryptography.

The security of the ECIES algorithm relies on the elliptic curve discrete logarithm problem, which involves the difficulty of solving discrete logarithms on elliptic curves. In implementation, different elliptic curves, base points, and symmetric encryption algorithms can be chosen to enhance security and efficiency. ECIES offers strong encryption protection while having shorter key lengths, efficient encryption and decryption speeds, and smaller data transmission sizes.

3. System Model

3.1. Overall Architecture

The system model, as illustrated in Figure 2, encompasses lightweight devices, capability devices, blockchain, users, homeowners, and mobile terminal apps.

- Lightweight devices: Typically, these are sensor devices in smart homes, such as smart meters and surveillance devices. These devices have limited resources, which is why we collectively refer to them as lightweight devices in this paper. The primary responsibility of lightweight devices is to provide services when accessed by users.
- Capability devices: These devices in smart homes possess sufficient computing, storage, and communication resources, including gateways, computers, and smart voice assistants. Capability devices not only provide services to users but also have the responsibility of maintaining the blockchain ledger.
- Blockchain: The blockchain is collectively maintained by all capability devices in the network. It deploys smart contracts and maintains lists, such as the decentralized identifier (DID) management table and the blockchain account address table. Each device in the network is assigned a blockchain account to record its activities within the system.
- Homeowners: Referring to the owners of smart homes, homeowners have higher security requirements in this model. They are primarily responsible for actions such as applying for DIDs for smart devices and issuing tokens. Homeowners possess a blockchain account and can perform corresponding operations using their account.
- Users: This refers to household members and visitors who may have resource demands on smart devices within the smart home.
- Mobile terminal app: This is a terminal application through which users interact with the blockchain network and request device services. This application enables convenient control and management of smart devices while ensuring system security.

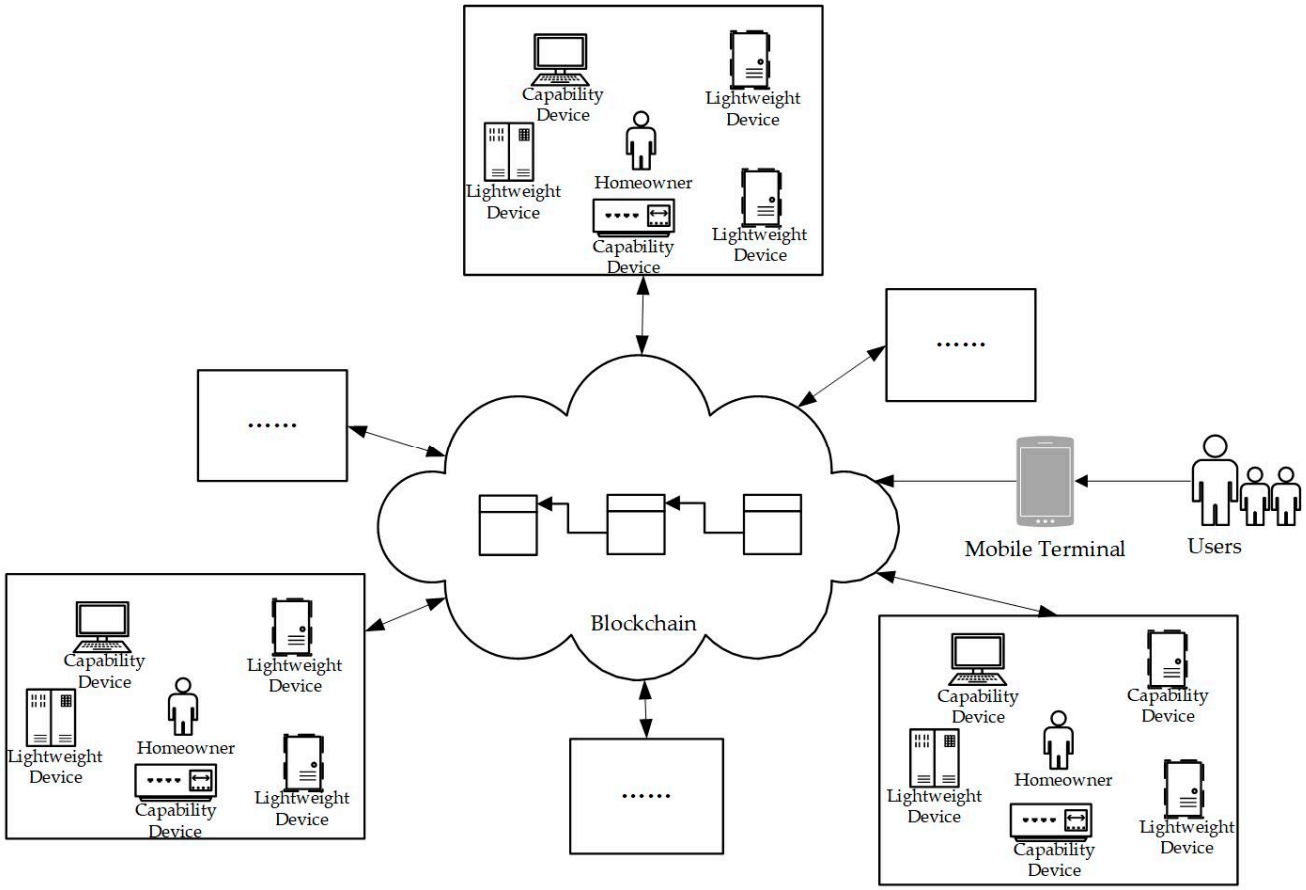

Figure 2. System model.

3.2. Smart Contract Module

Smart contracts [25] serve as the cornerstone for implementing various logical transactions on the blockchain. In this system, contracts are divided into the following main modules:

- DID Registration Contract: This contract enables users to apply for the generation of corresponding DDO documents based on their blockchain account address and attribute information, which are then stored in the DID management table. In the system proposed in this paper, there are two main types of DDOs, namely device DDOs and user DDOs, as illustrated in Figure 3.
- Account Application Contract: This contract allows devices, users, or homeowners to apply for a blockchain ledger key, which, when hashed, can generate a blockchain account address. Each account address will be stored in the blockchain account address list for other contracts to recognize and invoke. The contract ensures that each entity has a unique account address and enables quick lookup and access through the account address list.
- DID Query Contract: This contract provides users with a convenient encapsulated interface for querying the DID of the target device. Through this contract, users can input the device's name or other identifiers and obtain the corresponding DID. This contract facilitates users in finding the desired devices more easily and accelerates the overall system interaction process.
- DID Resolver Contract: When it is necessary to obtain the target information of an entity for an interaction, the DDO of the target DID can be acquired through this contract. Any malicious requests attempting to manipulate the DDO of others will be rejected, as only the DID owner can use this contract to obtain their DDO. This contract ensures that only authorized entities can access the information of other entities.

- DDO Update Contract: This contract allows entities to update their information when necessary, such as changing ownership, adding new features, or fixing defects. Only the owner of the DID can use the contract to update their DDO. The updating of Device DDOs falls under the rights of their respective owners. Through this contract, the system can ensure the accuracy and integrity of device information and prevent unauthorized modifications.
- DID Revocation Contract: If necessary, this contract can be used to delete the corresponding DDO and mark the DID as revoked. This functionality can also help protect information within the system. For instance, in the event of device theft or loss, the contract can be used to delete the device's DID, thereby safeguarding the device's information from unauthorized access.
- Token Issuance Contract: This contract allows the account owner to issue user tokens to users and permits the capability device D_c (see Section 4.1) to issue device capability tokens to users. These tokens will be used to authenticate the identities and permissions of users and devices. The token issuance contract requires the authentication of the user issuing the token and determines the type and validity period of the token based on the user's identity and permissions.
- Token Verification Contract: This contract is utilized to verify the legitimacy of user and device tokens. When a user makes an access request to a device, the token validation contract needs to parse the token, examine its validity and permissions, and based on the examination results, determine whether to permit the operation. If the token is invalid or lacks sufficient permissions, the request will be denied.

(**a**) (**b**)

Figure 3. Example of DDOs. (**a**) Example of device DDO. (**b**) Example of user DDO.

4. Solution Design

This section provides a detailed description of the proposed solution, which is based on decentralized identifiers (DIDs) for authentication and access control in the context of smart homes. The solution consists of four phases: system initialization, registration, authentication, and authorized access.

4.1. System Initialization Phase

During the system initialization phase, the blockchain network is maintained collaboratively by multiple capable devices in smart homes, and smart contracts are deployed on the blockchain. Subsequently, by invoking the Account Application contract, blockchain accounts are assigned to all smart devices and homeowners, and blockchain account address lists and DID management lists are maintained on the blockchain. By the completion of system initialization, the blockchain account addresses of all smart devices and homeowners are recorded in the account address list. The DID management list is initially empty, and its contents will be continuously updated during subsequent registration and other stages.

At the same time, in the system initialization phase, the proposed scheme requires the homeowner to select a capability device, denoted as D_c (typically the device with the highest computing, storage, and communication resources). D_c chooses an elliptic curve E, which is defined over a finite field F_ρ, satisfying the following equation:

$$y^2 = x^3 + ax + b(\text{mod } \rho) \tag{1}$$

where ρ is a prime number greater than 3, and $a, b \in F_\rho$ has a point G on it.

The system model employs elliptic curve integrated encryption to establish the shared key required for communication and utilizes the SHA256 hash algorithm to ensure data integrity during transmission.

4.2. Registration Phase

The registration phase consists of three components: special registration, device registration, and user registration.

4.2.1. Special Registration

Special registration includes the registration of the homeowner and D_c. After system initialization, both the homeowner and the smart devices have been assigned blockchain accounts. Due to the unique nature of the homeowner and D_c, they possess inherent trustworthiness during the registration phase. Simply submitting the blockchain account addresses to the DID registration contract allows the homeowner and D_c to be registered with their respective decentralized identifiers ($MDID$ and D_cDID) and stores their corresponding DDOs in the DID management list on the blockchain.

4.2.2. Device Registration

As indicated in Section 4.1, after system initialization, all homeowners and smart devices are assigned blockchain accounts. At this stage, homeowners can perform registrations using the blockchain account address of the corresponding device by invoking the DID registration contract. Once the device registration is successful, the blockchain network and D_c will generate a unique decentralized identifier (DDID) and its associated DID data object (DDO) for the device. The DDO will then be stored in the DID management list on the blockchain. The registration process for the i-th smart device is illustrated in Figure 4.

(a) D_c generates a random number r_i and a public key $PK_i = r_i \cdot G$, which is then sent to the registering device.

(b) The registering device generates a random number d_i and computes $R_i = d_i \cdot G$ and $S_i = d_i \cdot PK_i$. Subsequently, it sends R_i to D_c.

(c) D_c determines the shared secret S_i as follows:

$$S_i = d_i \cdot PK_i = d_i \cdot (r_i \cdot G) = r_i \cdot (d_i \cdot G) = r_i \cdot R_i \tag{2}$$

(d) The registering device uses its own blockchain account private key SK_{Device}. First, it calculates the blockchain account address $ACC_{Device} = H(SK_{Device})$ using the SHA256 hash function. Then, it encrypts ACC_{Device} with the shared secret S_i, resulting in $Enc(S_i, ACC_{Device})$, which is sent to D_c.

(e) Upon receiving the message, D_c decrypts $Enc(S_i, ACC_{Device})$ using the shared secret S_i. It then invokes the contract to query whether the homeowner's blockchain account address ACC_{Device} is present in the blockchain account address list. If it exists, D_c proceeds to register the $DDID$ for the registering device using the DID registration contract and stores the corresponding DDO in the DID management list. Otherwise, the request is rejected, and the connection is terminated.

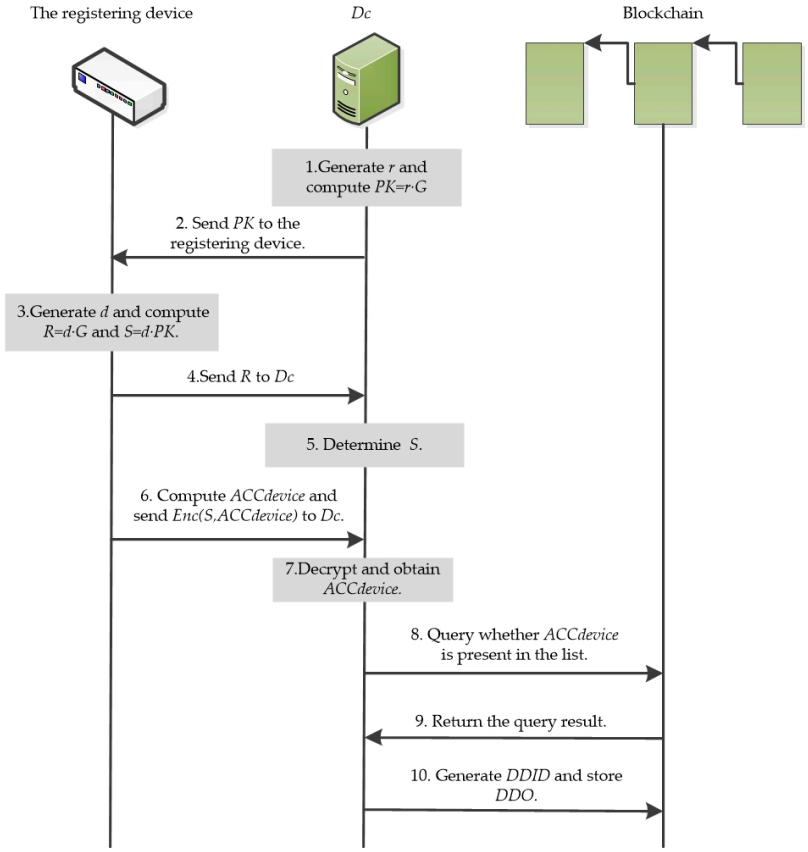

Figure 4. Device registration.

4.2.3. User Registration

Similarly, users utilize their assigned blockchain account addresses for registration, generating their decentralized identifier ($UDID$). The contract generates the user's DDO and stores it in the DID management list on the blockchain. The registration process for the j-th user is illustrated in Figure 5.

(a) Dc generates a random number r_j and computes the public key $PK_j = r_j \cdot G$, then sends PK_j to the user.

(b) The user generates a random number d_j, and computes $R_j = d_j \cdot G$ and $S_j = d_j \cdot PK_j$. Subsequently, the user sends R_j to D_c.

(c) D_c determines the shared secret key S_j as follows:

$$S_j = d_j \cdot PK_j = d_j \cdot (r_j \cdot G) = r_j \cdot (d_j \cdot G) = r_j \cdot R_j \tag{3}$$

(d) The user applies for a blockchain account private key SK_{User} through the account application contract to the blockchain, and the blockchain account address ACC_{User} is stored in the blockchain account address list.

(e) The user computes $H(SK_{User})$ using the SHA256 hash function and encrypts SK_{User} with the shared key S_j, resulting in $Enc(S_j, SK_{User})$. Subsequently, the user sends it to D_c.

(f) Upon receiving the message, D_c decrypts $Enc(S_j, SK_{User})$ using S_j and checks if the blockchain account address ACC_{User} is present in the blockchain account address list. If it exists, D_c registers a decentralized identifier $UDID$ for the account owner by invoking the DID registration contract and stores the corresponding DDO in the DID management list. Otherwise, D_c rejects the request and terminates the connection.

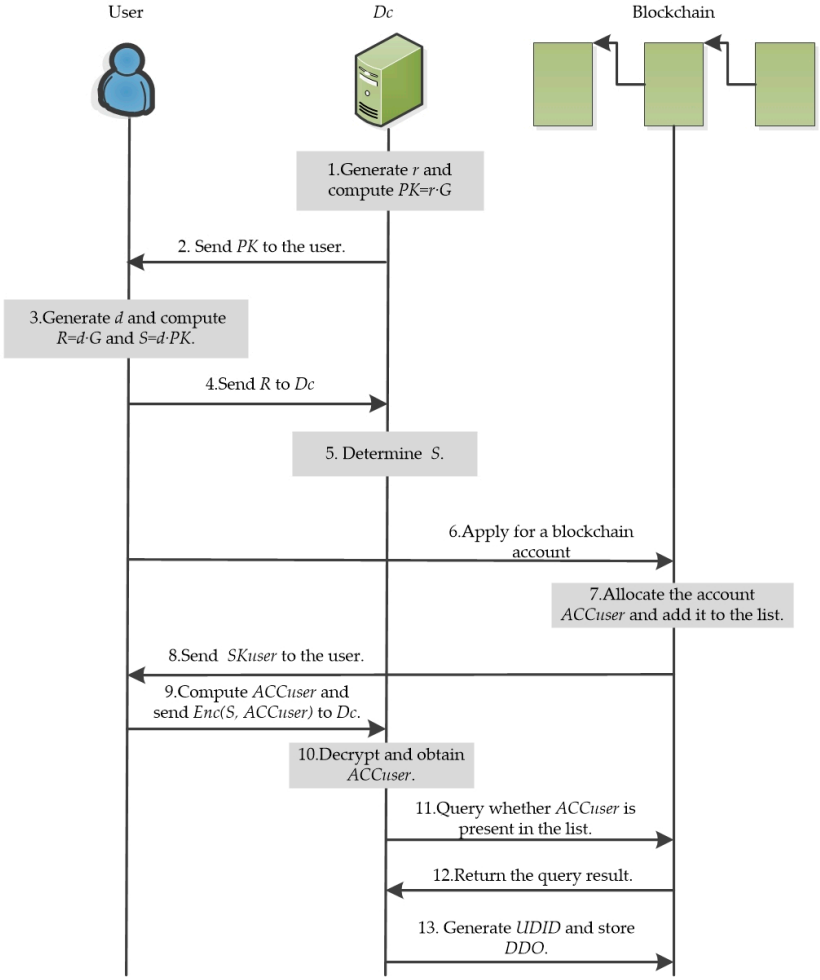

Figure 5. User registration.

4.3. Identity Authentication Phase

The process of identity authentication is illustrated in Figure 6.

If users need to access specific device services, they must undergo authentication before accessing the services. The detailed authentication process is as follows:

(a) Users enter the blockchain network through a mobile terminal app and invoke the DID query contract to locate the target device's $DDID$.

(b) The DID resolution contract is called to obtain the DDO identified by the $DDID$ Users can initiate an access request to the homeowner of the smart home where the device is located.

(c) Upon receiving the access request, the homeowner invokes the DID query contract to find the user's $UDID$ and then calls the DID resolution contract to learn about the user's specific details. The homeowner can choose whether to agree to provide access services. If agreed, the token issuance contract is called to issue a $token_{user}$, as shown below:

$$token_{user} \rightarrow \{MDID, UDID, T, TS, Sig\} \tag{4}$$

where,

$MDID$: The registered DID of the homeowner;
$UDID$: The registered DID of the user;
T: The time period during which the user token is valid;
TS: The timestamp at which the device token is generated;

Sig: The signature of the homeowner on the above attributes, which indicates that the user has completed authentication.

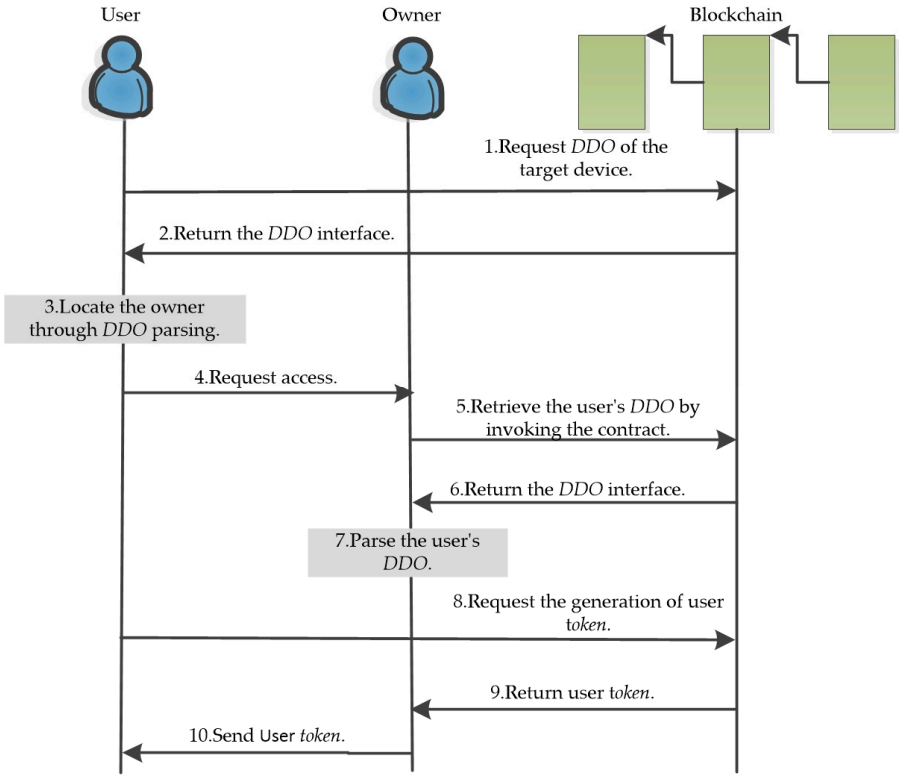

Figure 6. Identity authentication.

4.4. Authorized Access Phase

The process of authorized access is illustrated in Figure 7.

After successful user authentication, the user is issued a user token by the homeowner. Within the specified timeframe, the user can initiate access requests to the devices within the smart home using this token. The user is required to resolve the corresponding device's DDO to acquire D_c within the smart home and apply for the corresponding device's $token_{capability}$ from it. D_c verifies the $token_{user}$ by invoking the token validation contract to determine if the $token_{user}$ carried by the user has expired. If the token has expired, the request will be rejected. Otherwise, the capability device will grant the user the $token_{capability}$ for the device. The $token_{capability}$ is as follows:

$$token_{capability} \rightarrow \{UDID, DDID, AR, T, TS\} \tag{5}$$

where:

$UDID$: The user's registered DID;

$DDID$: The registered DID of the target device;

AR: Access rights for specific device services;

T: The validity period of the device capability token;

TS: The timestamp at which the device capability token is generated.

Once the $token_{capability}$ is obtained by the user, an access request can be initiated toward the target device. The token verification contract is invoked by the target device to validate the expiration of the token. If it is expired, the request is rejected; otherwise, the device verifies if it can provide the services specified in the token. If it cannot, an error is returned; otherwise, the device provides access to device services for the user.

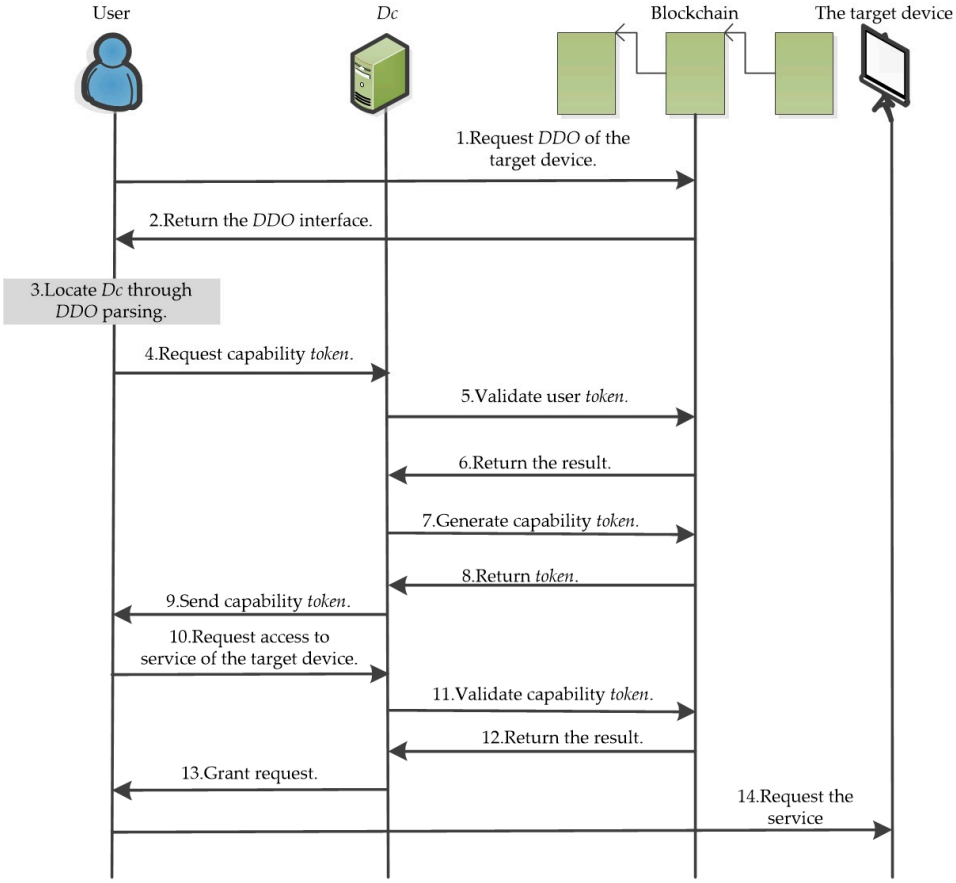

Figure 7. Authorized access.

In the proposed model, each participant (i.e., the user and the smart device) is assigned a unique DID. The access control permissions for specific device services are determined by the $token_{capability}$. As long as the user passes the identity authentication, they can initiate access requests to any device within the smart home. When the token expires, the user only needs to initiate the authentication process again.

5. Experimental Analysis

5.1. Security Analysis

The following assumes that the capability devices in the smart home are honest and trustworthy.

Lemma 1. *Assuming that the elliptic curve used in the scheme possesses cryptographic security, in which one-way security refers to the inability to obtain the corresponding plaintext from the ciphertext without knowing the private key. In other words, the probability of adversary A successfully reversing the encryption algorithm Enc can be considered negligible:*

$$Succ_A = P_r[(PK, SK) \leftarrow KG(\lambda) : A(PK, Enc(PK, m)) = m] \quad (6)$$

Proof of Lemma 1. When an attacker intercepts the public key PK and R in the transmission channel, he intends to solve for r and d separately, which is equivalent to solving the elliptic curve discrete logarithm problem. For instance, it is easy to compute $r \cdot G = PK$ given r, but calculating the corresponding r through PK is extremely difficult. Research has shown that the probability of solving this problem is extremely low and can be considered negligible. When the adversary cannot solve for r, he is also unable to obtain the shared secret key S.

Therefore, the probability P_A of the adversary successfully recovering the plaintext ACC from the ciphertext $Enc(S,\ ACC)$ is as follows:

$$P_A = P_r[(PK, SK) \leftarrow KG(G) : A(PK, Enc(PK, ACC)) = ACC] \tag{7}$$

According to the lemma, it can be inferred that P_A is negligible. Thus, the scheme achieves one-way security. □

In addition, the proposed scheme is capable of withstanding various attacks and possesses security features, such as tamper resistance.

- Replay Attack Resistance: In this system, D_c generates a new key pair for each session request, which is used for encrypting response messages and computing messages. Since the generated key pair is always up to date, it can withstand any replay attacks. Additionally, during the authentication and authorization access phase, timestamps are included in the user token and device capability token, ensuring full resistance against replay attacks.
- Impersonation Attack Resistance: The system adopts a decentralized identifier (DID) to authorize legitimate user access, and due to the uniqueness of each object's DID, it is impossible for any unauthorized user to impersonate others.
- Man-in-the-Middle Attack Resistance: Decentralized identifiers (DIDs) are distributed across multiple nodes, eliminating the reliance on a single centralized authority and significantly reducing the risk of unauthorized interception and manipulation of communication. The process of storing and verifying DIDs involves rigorous identity authentication, leveraging cryptographic techniques such as digital signatures and public-key encryption. These measures effectively prevent impersonation by intermediaries, ensuring the integrity and authenticity of the communication channels.
- Denial-of-Service (DoS) Attack Resistance: Due to the token verification contract performing token expiration and validity checks for each request, the system can avoid DoS attacks and ensure smooth operation.
- Malicious Node Attack Resistance: The system is implemented using blockchain technology, guaranteeing the immutability and decentralization of the distributed ledger, which effectively mitigates attacks from malicious nodes.
- Tamper Resistance: Firstly, without a valid token, attackers are unable to access data through access requests. Secondly, all data stored on the blockchain are formed into a Merkle tree to create a hash value, and the blocks are linked together through hash values, contributing to the robust tamper-resistant capability of the blockchain. Both types of tokens are stored on the blockchain, which prevents unauthorized modification by attackers.
- Traceability: All critical information is preserved in an immutable distributed ledger on the blockchain, enabling the tracing of any malicious activities and reducing improper behavior by malicious users.
- Confidentiality: The services provided by the devices are protected and accessed only by two parties: the homeowner and the user. It is at the discretion of the homeowner to issue user tokens to specific individuals, and unauthorized individuals are prohibited from using the smart device services without the homeowner's approval.
- Integrity: Hash functions possess irreversibility, uniqueness, and collision resistance, significantly reducing the possibility of data forgery and enabling the precise tracking and verification of recorded data. All DIDs, DDOs, and tokens are stored on the blockchain, preventing arbitrary manipulation and ensuring the integrity of the system.

In order to assess the security of the proposed smart home access control scheme, a comparison was made to several other schemes in terms of security aspects, as shown in Table 1:

Table 1. Comparison of the schemes.

Security Feature	[12]	[20]	[22]	Proposed Scheme
Confidentiality	√	×	√	√
Tamper Resistance	×	√	×	√
Traceability	×	√	×	√
Scalability	×	×	√	√
Integrity	√	√	√	√

In this table, a checkmark (√) indicates the presence of a particular security feature in a given scheme, while a cross (×) indicates its absence.

5.2. Performance Analysis

In this study, we selected Ethereum [26] as the smart contract platform and utilized the Solidity language for contract development. For the convenience of contract testing and deployment, we employed the Remix0.34.1 integrated development environment and the Truffle framework. Additionally, we utilized the Web3.js library for interacting with Ethereum nodes. To simulate the Ethereum network environment, we employed Ganache 2.7.1 as the local testing node [27]. During the contract development process, we utilized the ERC725 standard contract provided by the open-source library OpenZeppelin to implement the functionality of decentralized identifiers. OpenZeppelin is a widely used Ethereum smart contract library that offers audited and security-tested contracts to assist developers in building more secure and reliable smart contracts. By employing the aforementioned tools and technologies, we realized the proposed smart home solution outlined in this paper and conducted experimental validation. The experimental environment is summarized in Table 2.

Table 2. Experimental environment.

Software/Hardware	Parameter
Operating system	Ubuntu Linux 20.04LTS
CPU	AMD Ryzen 7 4800H with Radeon Graphics
Programming Language	solidity0.8.0
Memory	16 GB

To accurately assess the performance of the proposed scheme, we conducted measurement experiments on six key services, including DID registration, DID resolution, user token generation, user token verification, device capability token generation, and device capability token verification. Each service was tested 50 times, and the average values were computed for presentation, as shown in Figure 8. The longer average time cost of DID registration, user token generation, and device capability token generation, which reached 129 ms, 68 ms, and 62 ms, respectively, compared to the other three services, is because these three services involve blockchain transactions, in which multiple transactions are consecutively generated and stored in consecutive blocks, resulting in a longer execution time required for these services. However, it is worth noting that in typical scenarios, the DID registration service is only executed once, and the user token generation service is also executed once within a certain time frame. Each time a device is accessed, only the device capability token generation service needs to be executed. Overall, considering the advantages of decentralized identifiers, the incurred time cost is acceptable.

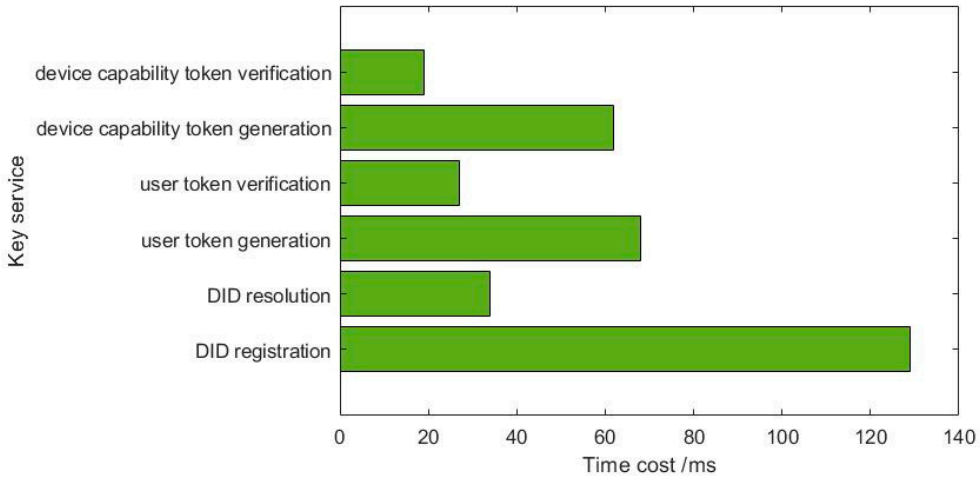

Figure 8. The average time cost of the six key services was obtained through 50 test runs. DID registration, user token generation, and device capability token generation involve blockchain transactions, resulting in relatively higher average time costs.

In addition, the response time of the proposed scheme was tested, which refers to the time required from sending an access request to receiving the authorization [28]. In our scheme, users only need to request the issuance of the $token_{user}$ once within a certain time period for access. To simulate real-world scenarios accurately, we tested the continuous access of different numbers of users (1, 3, 5, and 10) within the validity period of the $token_{user}$, as shown in Figure 9. It can be observed that regardless of the number of users, the response time for the first round of access requests is higher than that of the subsequent rounds. This is because the initial access requires user DID registration and $token_{user}$ application, resulting in a longer response time. However, for the subsequent rounds, which are within the validity period of the $token_{user}$, the response time is shorter and similar. Considering real-world smart home environments, users can enjoy device services quickly, securely, and repeatedly for a period of time after a relatively longer registration period, which aligns with the actual needs of smart home residents.

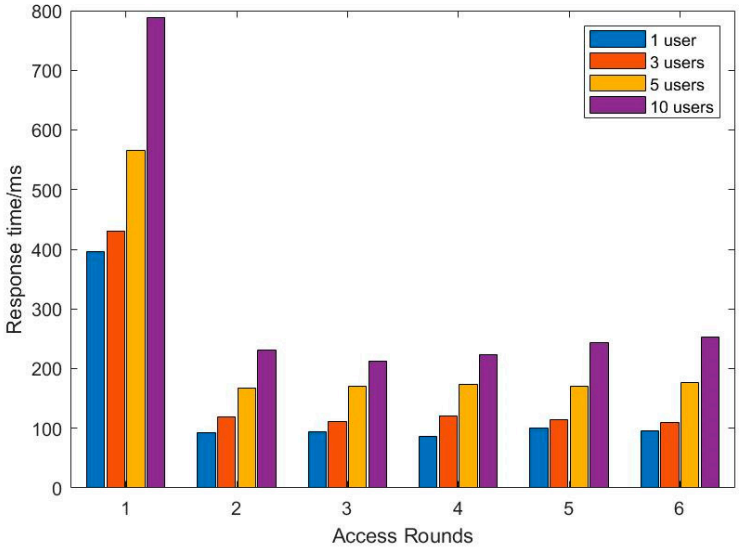

Figure 9. The response times of continuous access for different numbers of users (1, 3, 5, and 10) within the validity period of $token_{user}$ were measured. Except for the first round, which requires DID registration and application for user tokens, the response times for the subsequent rounds were relatively short and similar, aligning with the actual needs of smart home residents.

A comparison of the response times with those of other schemes is presented in Figure 10, where the number of access requests is set to 5/10/15/20/25/30, respectively. The scheme proposed in this paper outperforms the others due to its improved permission access control and DID-based authentication. In contrast, the centralized network architecture used in the literature [12] exhibits low response times initially but becomes insufficient to handle an increasing number of access requests. On the other hand, schemes presented in the literature [20,22] that employ distributed network architectures combined with blockchain suffer from progressively higher response times due to complex authentication processes.

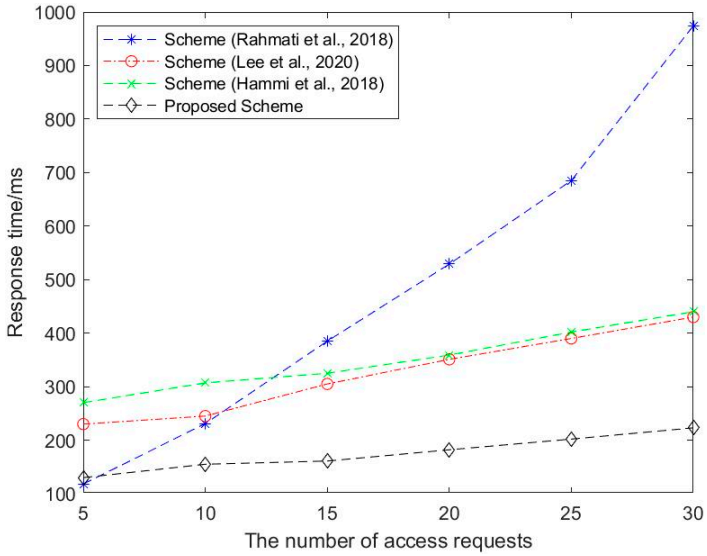

Figure 10. The response times of different schemes under varying numbers of access requests were compared. The centralized network architecture used in Scheme [12] experienced a significant increase in response time as the number of requests increased. While Schemes [20,22] remained relatively stable, they were not as prompt as the proposed scheme in terms of response speed.

Based on the tests conducted, it can be observed that the proposed solution is more suitable for scenarios in smart homes in which fixed users access device services multiple times within a specific time period, as opposed to scenarios in which new users access services once and then stop.

This paper also conducted tests on the communication cost, with the transmission bandwidth used to initiate an access request as the test value. The experimental results were obtained by averaging 10 test values. Similar to the response time experiments, a comparison was made with references [12,20,22], as shown in Figure 11. Reference [12] employed a centralized architecture, in which all communication passes through one or several central nodes or servers. As the data and instructions need to be transmitted through this central node, it faces a greater burden with an increase in communication volume, leading to a higher communication overhead, with an average of 2272.31 bits for 10 tests. Although the proposed scheme and references [20,22] adopt distributed architectures, the proposed approach mainly utilizes the computational and communication resources of the most capable devices within the smart home network for data processing and transmission, resulting in a lower transmission bandwidth and superior communication overhead, with an average of only 1261.97 bits for 10 tests.

Communication cost is crucial for smart home security solutions. Reducing communication overheads can enhance data transmission speed, ensure privacy protection, achieve real-time responsiveness, strengthen security authentication, ensure data integrity, and improve energy efficiency, thereby enhancing the overall security and reliability of the entire smart home system.

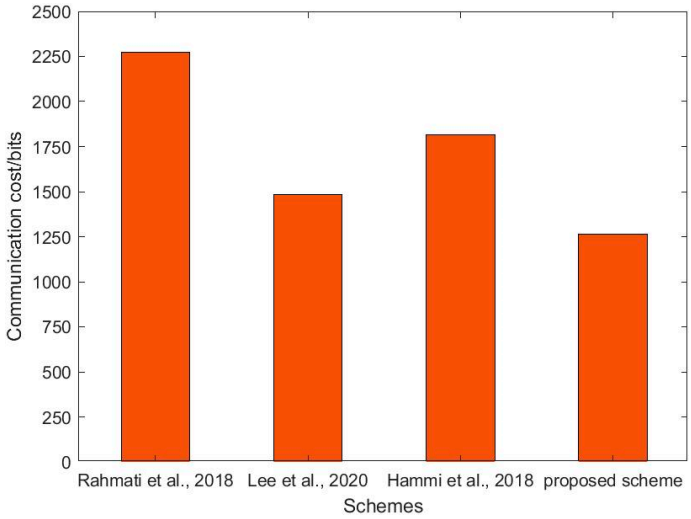

Figure 11. The proposed scheme is compared with the communication cost of the schemes presented in references [12,20,22]. The proposed approach, being a distributed architecture and primarily utilizing the computational and communication resources of the most capable devices within the smart home network for data processing and transmission, exhibits superior communication overhead.

Similar to cloud computing, using blockchain resources also incurs corresponding costs. In Ethereum, transactions are charged using the gas mechanism [29], which serves as a measure of the computational cost of executing transactions or contracts. Ethereum employs a dedicated virtual machine to process transactions, and the virtual machine sequentially processes each operation instruction specified in the transaction. Each operation instruction has a predetermined gas consumption value explicitly defined. The gas consumption for some operations is shown in Table 3. As a result, the total gas required for transactions or contract execution depends on the included operations and their quantities.

Table 3. Gas consumption of certain operations.

Mnemonic	Gas Used	Notes
STOP	0	Halts execution.
ADD	3	Addition operation
MUL	5	Multiplication operation
SUB	3	Subtraction operation
DIV	5	Integer division operation
ADDMOD	8	Modulo addition operation
MULMOD	8	Modulo multiplication operation
BLOCKHASH	20	Get the hash of one of the 256 most recent complete blocks
BALANCE	400	Get balance of the given account
EXTCODESIZE	700	Get size of an account's code

In this study, we conducted tests to measure the gas consumption for executing basic functionalities in smart contract design and compared it with other Ethereum-based approaches, as shown in Figure 12. Clearly, our solution requires the least amount of gas compared to other methods, indicating a reduced number of operations and complexity. This demonstrates the lightweight nature of our approach, characterized by efficiency and simplicity. Its lightweight design offers advantages in processing speed and resource utilization, leading to reduced costs for executing solutions on the Ethereum network. Consequently, our solution can be considered an excellent lightweight approach suitable for scenarios that demand efficiency, simplicity, and cost-effectiveness, such as smart home systems.

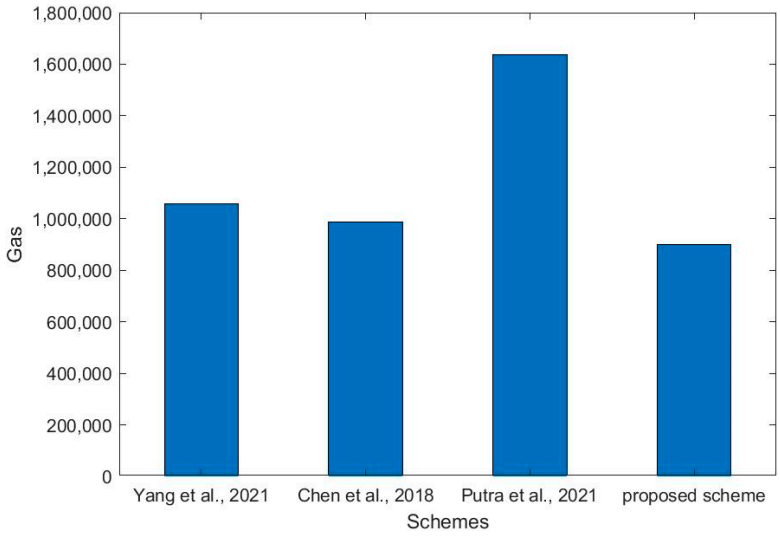

Figure 12. The comparison of gas consumption between the proposed approach and the schemes in the literature [23,25,29] is presented. The proposed solution exhibits the least gas consumption, indicating a reduced number of operations and decreased complexity, showcasing the lightweight nature of this approach.

6. Conclusions

In this paper, we address security issues related to identity authentication and access control in smart home systems by proposing a decentralized identifier-based approach. Our goal is to overcome the single point of failure problem in traditional centralized architectures while considering the balance between the resource constraints and security requirements of smart devices. Compared to traditional centralized architectures and existing distributed solutions, our proposed scheme leverages blockchain technology to achieve higher security while eliminating single points of failure. Furthermore, our approach combines decentralized identifiers with an improved capability-based access control policy, simplifying user identity authentication and enabling convenient access across multiple households with a one-time registration process. Our experimental results demonstrate that our proposed scheme performs excellently in terms of both security and performance. A comprehensive comparative analysis with other schemes proves that our decentralized identifier-based authentication and access control scheme strikes an outstanding balance between security and having a lightweight design, aligning well with the actual needs of smart home users and making it an excellent solution in the field of smart home security.

As smart cities rapidly evolve, smart homes are no longer limited to individual households, but can extend to entire neighborhoods or even entire counties under the same network. Our proposed solution, relying on blockchain technology, allows the security of smart home clusters to increase as their scale expands. However, this expansion also gives rise to other challenges, making scalability a primary focus of future research.

Author Contributions: Conceptualization, X.Z. and B.Z.; methodology, X.Z.; software, X.Z.; validation, X.Z., B.Z. and Z.C.; formal analysis, X.Z.; investigation, X.Z. and Z.C.; resources, X.Z. and B.Z.; data curation, X.Z. and Z.C.; writing—original draft preparation, X.Z.; writing—review and editing, X.Z., B.Z. and Z.C.; visualization, X.Z.; supervision, B.Z.; project administration, B.Z.; funding acquisition, B.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Natural Science Foundation of China Youth Science Foundation Project (No. 62102241).

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Acknowledgments: The authors would like to acknowledge the Shanghai University of Engineering Science for its lab facilities and necessary technical support.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660.
2. da Ponte, F.R.; Gomes, R.L.; Celestino, J.; Madeira, E.R.; Patel, A. IoT device programmable language customization for home automation. In Proceedings of the 2018 IEEE Symposium on Computers and Communications (ISCC), Natal, Brazil, 25–28 June 2018; pp. 168–173.
3. Padmanaban, S.; Nasab, M.A.; Shiri, M.E.; Javadi, H.H.S.; Nasab, M.A.; Zand, M.; Samavat, T. The role of internet of things in smart homes. In *Artificial Intelligence-based Smart Power Systems*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2023; pp. 259–271.
4. Kavallieratos, G.; Chowdhury, N.; Katsikas, S.; Gkioulos, V.; Wolthusen, S. Threat Analysis for Smart Homes. *Future Internet* **2019**, *11*, 207. [CrossRef]
5. Schiansky, P.; Kalb, J.; Sztatecsny, E.; Roehsner, M.-C.; Guggemos, T.; Trenti, A.; Bozzio, M.; Walther, P. Demonstration of quantum-digital payments. *arXiv* **2023**, arXiv:2305.14504.
6. Yin, H.-L.; Fu, Y.; Li, C.-L.; Weng, C.-X.; Li, B.-H.; Gu, J.; Lu, Y.-S.; Huang, S.; Chen, Z.-B. Experimental quantum secure network with digital signatures and encryption. *Natl. Sci. Rev.* **2023**, *10*, nwac228. [PubMed]
7. Pereira, M.; Currás-Lorenzo, G.; Navarrete, Á.; Mizutani, A.; Kato, G.; Curty, M.; Tamaki, K. Modified BB84 quantum key distribution protocol robust to source imperfections. *Phys. Rev. Res.* **2023**, *5*, 023065.
8. Gu, J.; Cao, X.-Y.; Fu, Y.; He, Z.-W.; Yin, Z.-J.; Yin, H.-L.; Chen, Z.-B. Experimental measurement-device-independent type quantum key distribution with flawed and correlated sources. *Sci. Bull.* **2022**, *67*, 2167–2175.
9. Kang, W.M.; Moon, S.Y.; Park, J.H. An enhanced security framework for home appliances in smart home. *Hum. -Centric Comput. Inf. Sci.* **2017**, *7*, 6.
10. Wu, T.-Y.; Meng, Q.; Chen, Y.-C.; Kumari, S.; Chen, C.-M. Toward a Secure Smart-Home IoT Access Control Scheme Based on Home Registration Approach. *Mathematics* **2023**, *11*, 2123. [CrossRef]
11. Haseeb-ur-Rehman, R.M.A.; Liaqat, M.; Aman, A.H.M.; Almazroi, A.A.; Hasan, M.K.; Ali, Z.; Ali, R.L. LR-AKAP: A Lightweight and Robust Security Protocol for Smart Home Environments. *Sensors* **2022**, *22*, 6902.
12. Rahmati, A.; Fernandes, E.; Eykholt, K.; Prakash, A. Tyche: Risk-based permissions for smart home platforms. *arXiv* **2018**, arXiv:1801.04609.
13. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. LSB: A Lightweight Scalable Blockchain for IoT security and anonymity. *J. Parallel Distrib. Comput.* **2019**, *134*, 180–197.
14. Yakubu, B.M.; Khan, M.I.; Bhattarakosol, P. IPChain: Blockchain-Based Security Protocol for IoT Address Management Servers in Smart Homes. *J. Sens. Actuator Netw.* **2022**, *11*, 80. [CrossRef]
15. Singh, S.; Ra, I.-H.; Meng, W.; Kaur, M.; Cho, G.H. SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology. *Int. J. Distrib. Sens. Netw.* **2019**, *15*, 1550147719844159. [CrossRef]
16. Menon, S.; Anand, D.; Kavita; Verma, S.; Kaur, M.; Jhanjhi, N.Z.; Ghoniem, R.M.; Ray, S.K. Blockchain and Machine Learning Inspired Secure Smart Home Communication Network. *Sensors* **2023**, *23*, 6132.
17. She, W.; Gu, Z.-H.; Lyu, X.-K.; Liu, Q.; Tian, Z.; Liu, W. Homomorphic consortium blockchain for smart home system sensitive data privacy preserving. *IEEE Access* **2019**, *7*, 62058–62070.
18. Zeng, Y.; Wei, L.; Cheng, Y.; Zhang, H.; Sun, W.; Wang, B. Blockchain-Enabled Intelligent Dispatching and Credit-Based Bidding for Microgrids. *Electronics* **2023**, *12*, 2868. [CrossRef]
19. Liu, Y.; Lu, Q.; Chen, S.; Qu, Q.; O'Connor, H.; Choo, K.-K.R.; Zhang, H. Capability-based IoT access control using blockchain. *Digit. Commun. Netw.* **2021**, *7*, 463–469. [CrossRef]
20. Lee, Y.; Rathore, S.; Park, J.H.; Park, J.H. A blockchain-based smart home gateway architecture for preventing data forgery. *Hum. Centric Comput. Inf. Sci.* **2020**, *10*, 9.
21. Matsumoto, N.; Kotani, D.; Okabe, Y. Capability Based Network Access Control for Smart Home Devices. In Proceedings of the 2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), Pisa, Italy, 21–25 March 2022; pp. 551–556.
22. Hammi, M.T.; Hammi, B.; Bellot, P.; Serhrouchni, A. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Comput. Secur.* **2018**, *78*, 126–142.
23. Yang, X.; Yang, X.; Yi, X.; Khalil, I.; Zhou, X.; He, D.; Huang, X.; Nepal, S. Blockchain-based secure and lightweight authentication for Internet of Things. *IEEE Internet Things J.* **2021**, *9*, 3321–3332.
24. Shao, S.-F.; Cao, X.-Y.; Xie, Y.-M.; Gu, J.; Liu, W.-B.; Fu, Y.; Yin, H.-L.; Chen, Z.-B. Experimental Phase-Matching Quantum Key Distribution without Intensity Modulation. *arXiv* **2023**, arXiv:2303.11585.
25. Chen, Y.-D.; Azhari, M.Z.; Leu, J.-S. Design and implementation of a power consumption management system for smart home over fog-cloud computing. In Proceedings of the 2018 3rd International Conference on Intelligent Green Building and Smart Grid (IGBSG), Yilan, Taiwan, 22–25 April 2018; pp. 1–5.

26. Hossain, S.; Waheed, S.; Rahman, Z.; Shezan, S.; Hossain, M.M. Blockchain for the security of internet of things: A smart home use case using ethereum. *Int. J. Recent Technol. Eng.* **2020**, *8*, 4601–4608. [CrossRef]
27. Ch, R.; Kumari, D.J.; Gadekallu, T.R.; Iwendi, C. Distributed-Ledger-Based Blockchain Technology for Reliable Electronic Voting System with Statistical Analysis. *Electronics* **2022**, *11*, 3308. [CrossRef]
28. Liu, X.; Huang, Z.; Wang, Q.; Wan, B. An Evolutionary Game Theory-Based Method to Mitigate Block Withholding Attack in Blockchain System. *Electronics* **2023**, *12*, 2808. [CrossRef]
29. Putra, G.D.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R.; Ignjatovic, A. Trust-based blockchain authorization for iot. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 1646–1658. [CrossRef]